Energy Provider Community of Interest
February 2, 2016

Securing Networked Infrastructure for the Energy Sector

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

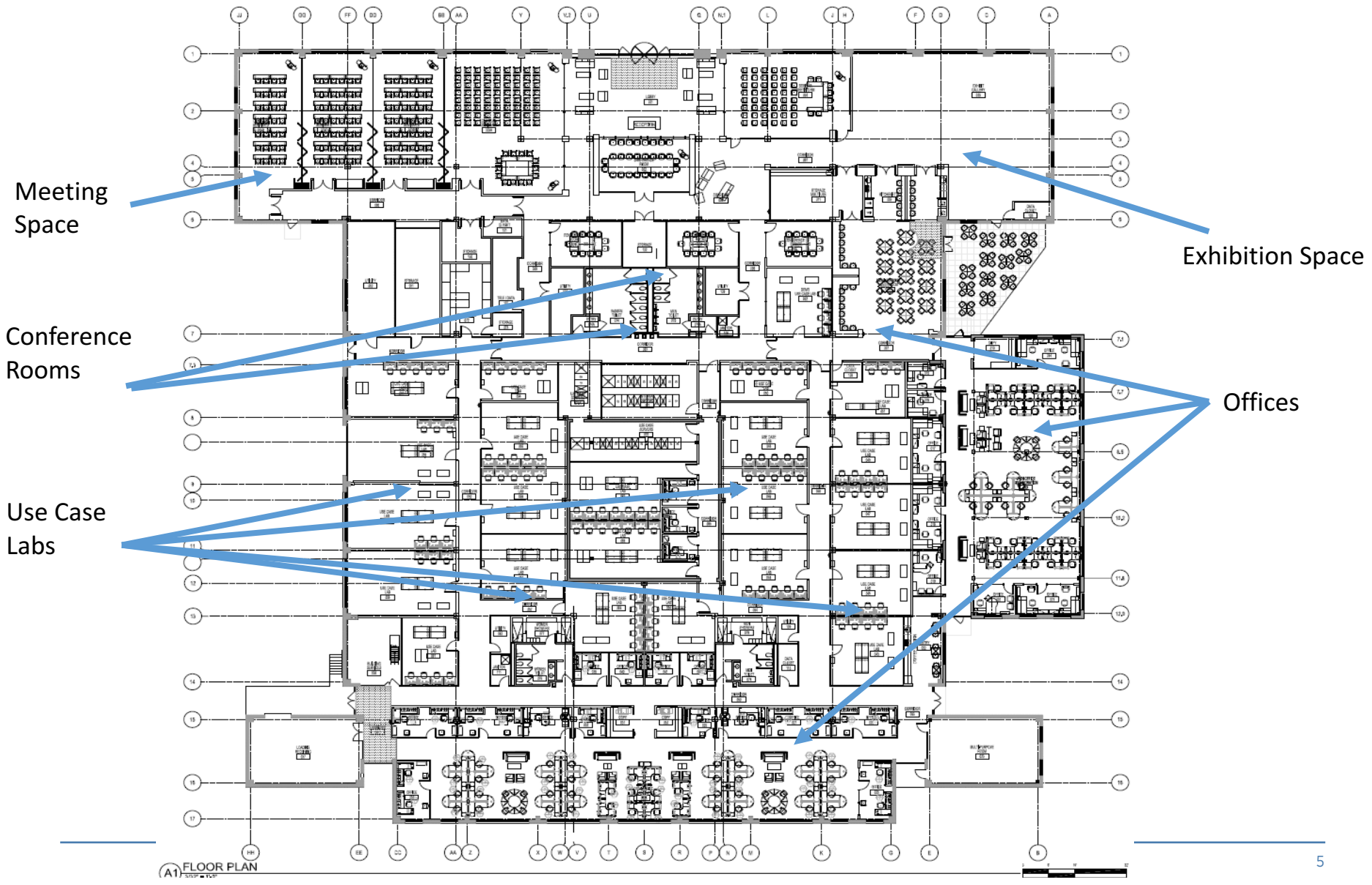
- NCCoE News
- Current Project Overview
  - Identity and Access Management (IdAM) project update
  - Situational Awareness (SA) project update
- Open Discussion

We moved!

- New physical address: 9700 Great Seneca Hwy, Rockville, MD 20850
- New shipping address: 100 Bureau Drive, Mail Stop 2002, Gaithersburg, MD 20899

NEW LOCATION (ROCKVILLE, MD)

NCCOE FACILITY

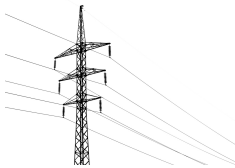


NCCoE Out and About:

- Upcoming planned conferences
  - RSA (Feb)
  - UTC & Technology (May)
  - ICS JWG (May)
  - APPA (June)
  - EnergySec (August)
  - ICS Europe (September)
  - ICS Sacramento (October)
  - GridSecCon (October)
- Upcoming planned visits
  - Black & Veatch, Western Farmers Electric Cooperative

Identity and Access Management (IdAM) Use Case:

Converged management of silos



- Provides a reference solution to:
  - Authenticate individuals and systems
  - Enforce authorization control policies
  - Unify IdAM services
  - Protect generation, transmission and distribution
  - Improve awareness and management of visitor accesses
  - Simplify the reporting process
- Draft guide is online at https://nccoe.nist.gov/projects/use_cases/idam
- Final Guide publication in February/ March 2016 timeframe
- Demonstrations available in NCCoE lab or on site

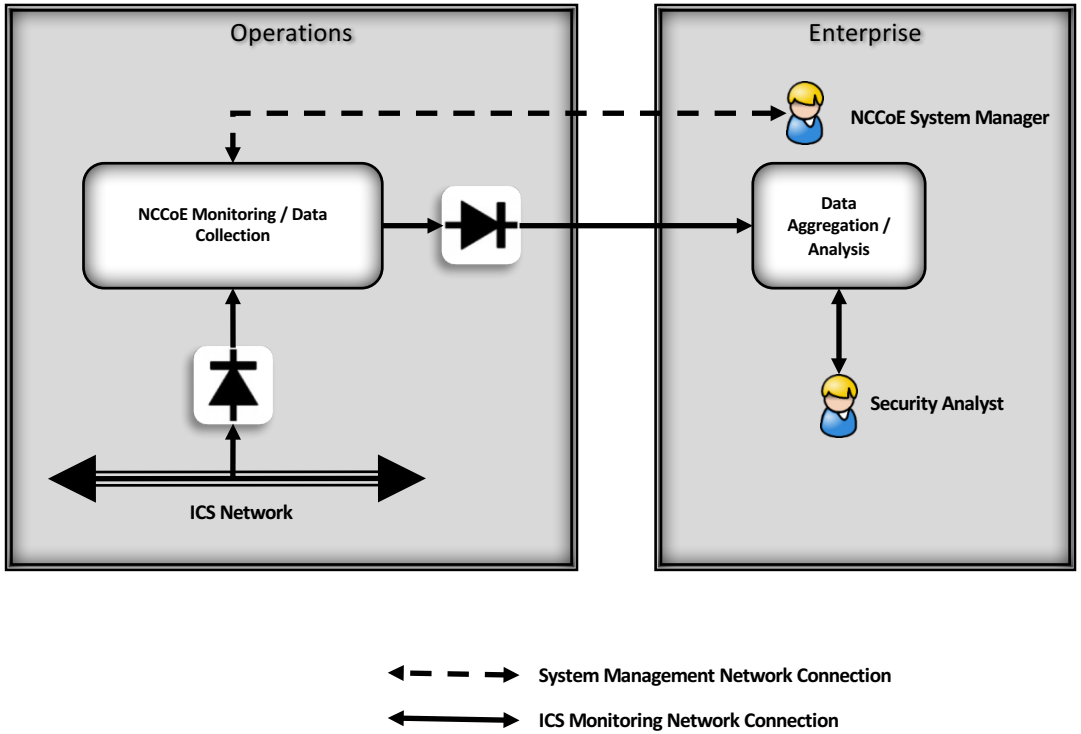
IdAM Adoption Activities

- Continue to seek early adoption opportunities
- Increased engagement with industry utilities and integrators
- Opportunities for COI members:
  - Demonstration of solution for your organization
  - Solution feasibility discussions
  - Industry vendor/ integrator introductions
  - COI outreach support

Contact us to join the pilot program!

Situational Awareness Project

- Improve OT availability
- Detect anomalous conditions and remediation
- Investigate events leading to anomalies and share findings
- Unify visibility across silos

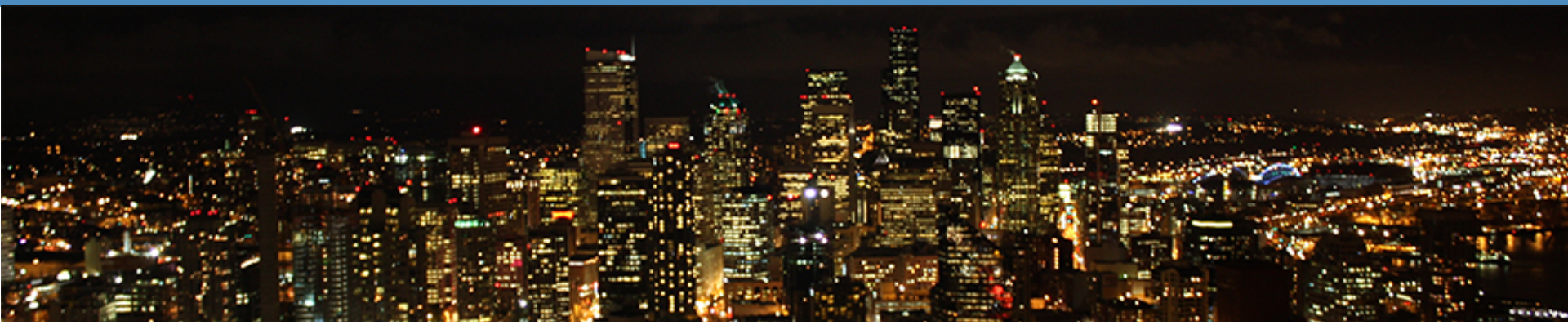


Situational Awareness Project Milestones

- Use Case published: http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Situational_Awareness.pdf
- Build team kickoff: 10/20/2015
- Components installed in lab: 12/2015
- Systems integration in new lab: 1/2016 – 3/2016
- Draft Practice Guide release: 3/2016
- Early adoption: 3/2016 and ongoing
- Demonstrations: 4/2016 and ongoing
- Final Practice Guide release: 6/2016

Date driven by desire to support NERC CIP compliance date of 1 April

OPEN DISCUSSION



- We are investigating the use of Model-Based Systems Engineering (MBSE) as part of our reference solution development process
  - MBSE would create SysML models that could be published along with Practice Guides
- Questions for the community
  - Does your company use Model-Based Systems Engineering?
    - http://www.omgwiki.org/MBSE/doku.php
  - Would SysML models facilitate adoption of NCCoE reference solutions by your company?
    - http://www.omgsysml.org/#What-Is_SysML

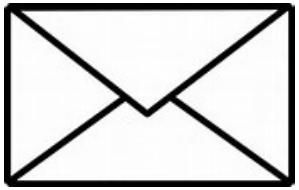
CONTACT US

240-314-6800

http://nccoe.nist.gov/forums/energy

energy_nccoe@nist.gov

9700 Great Seneca Hwy,
Rockville, MD 20850



100 Bureau Drive, Mail Stop
2002, Gaithersburg, MD 20899

Thank You

ABOUT THE NCCOE

National Institute of Standards and Technology
U.S. Department of Commerce

Information Technology Laboratory

MARYLAND OF OPPORTUNITY.®
Department of Business & Economic Development

MONTGOMERY COUNTY
17 76
GARDEZ BIEN
MARYLAND

WHO WE ARE AND WHAT WE DO

VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

The NCCoE seeks problems that are:

- Broadly applicable across much of a sector, or across sectors
- Addressable through one or more reference designs built in our labs
- Complex enough that our reference designs will need to be based on a combination of multiple commercially available technologies

Reference designs address:

- Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)

TENETS

Standards-based

Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards

Modular

Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions

Commercially available

Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry

Usable

Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results

PROJECT LIFECYCLE